Amendments to the Specification:

As indicated at page 4, lines 5-10, the present application incorporates by reference copending application entitled METHOD AND APPRATUS FOR A SECRUE REMOTE ACCESS SYSTEM, filed July 19, 2000, having attorney docket number MONG-00-002 (referred to herein as the "002 Application"). Applicant hereby expressly incorporates the following sections of the 002 Application in the present application.

At page 13, after the paragraph concluding at line 18, and prior to the paragraph beginning at line 20, please insert the following text (this text is taken from the 002 Application at page 8, line 18 – page 9, line 9; page 16, line 6 – page 17, line 20; page 27, line 9 – page 28, line 10; and page 31, line 4 – page 32, line 3 (reference numbers have been changed to conform to the present application)).

-- The invention provides a second secure channel between the user server module and the base device using a private protocol. To provide additional security, the invention provides that data communications between the user server module and the base device be initiated by the base device, rather than the server module. The details for carrying out communication transactions with the base device is described more fully below. In general, the base device initiates a request to the user server module which opens a communication socket between the base device and the user server module. In particular, the communication socket permits the base device and the user server module to communicate through a firewall. Once this communication socket is open, the server module is

able to issue commands to the base device. In response, the base device then executes the command.

The base devices typically connect to the Internet using conventional connection means, such as dial-up, cable, or network connections, for example. Each base device contains or provides an access gateway to information which is provided to the user of the remote access device. Such information may include, for example, computer files such as address book files, document files, email documents, among others. Each base device is identified with a user of the remote access device via conventional authentication means, such as challenge and response authentication. For example, when a remote user provides a user name and password to the system 10, the system 10 then identifies the base device which the user is entitled to access.

The base devices may be any conventional data processing means or computer suitable for communicating data to the user server modules 28 in accordance with the present invention. The "base" device and its operation is described in copending application entitled " AGENT SYSTEM FOR A SECURE REMOTE ACCESS SYSTEM " having the attorney docket number MONG-00-003 and filed July 19, 2000, the disclosure of which is expressly incorporated herein by reference.

In cases where a base device does not have a permanent (i.e., persistent or "full-time") connection to the Internet, the Sili server 30 is configured to "wake-up" the base device. Normally, this process is carried out when a user identified with the base devices is accessing the system 10 via a remote access device. Accordingly, the system 10 may be further coupled to the base devices via the Sili server 30. The Sili server 30 is coupled to a modem pool which may comprise a bank or pool of modems as is known in the art. The Sili server 30 is configured to dial the base device by calling a phone number designated for the base device via PSTN (public switched telephone network) and negotiate a connection between the base device and Sili server via the Internet. During negotiation, the Sili server 30 typically identifies the identity (or location such as the IP address) of the Sili server 30, and then terminates the PSTN connection. In response, the base device then carries out the operation of connecting to the Internet and communicating with the Sili server 30 over the Internet connection. Once connected with the Sili server 30 via the Internet (whether permanently or as requested during the above described "wake up" process), the Sili server 30 then communicate which user server module is requesting data from the base device.

Preferably, communications between the base device and the Sili server 30 are initiated by the base device. For example, a base device which maintains a full time Internet connection is generally configured to periodically communicate "job request" commands at a predetermined interval (e.g., forty (40) seconds) to the Sili server 30. In response, the Sili server 30 may indicate "no job" or "job request

by a user server module". "No job" is communicated where the user associated with the base device is not requesting data at this time. "Job request by a user sever module" is communicated when the user associated by the base device is requesting data. Where the Sili server 30 indicates that a job request is pending, the Sili server 30 also identifies the particular user server module 28, normally by identifying the IP address of the particular user server module.

If the base device does not maintain a full-time Internet connection, further processing may be required to establish a communication between the Sili server 30 and the base device over the Internet. The Sili server 30 may readily determine whether a particular base device maintains a full time Internet connection by checking whether the base device communicates period "job request" commands as described above. Where the base device does not maintain a full-time connection to the Internet, the invention provides means for signaling the base device to establish an Internet connection and connect to the Sili server 30.

As described above, communication sequences between the system 10 (Sili server 30 and user server module 28) and the base device is generally initiated by the base device, rather than the system 10. However, for data transfers and key operations (such as file transaction), communications are initiated by the remote device. This arrangement provides several advantages which overcomes problems associated with the prior art. First, security is

increased since the data communications are initiated by the base device rather than by the system 10. By requiring the base device to initiate communication (and therefore establish a connection socket), hacking into the base device from the outside becomes a more difficult task. Additionally, the invention may be practiced even if the base device is behind firewall because the base device initiates communication and opens the connection to the agent communication module, thereby allowing reply communications and task commands to be communicated from the agent communication module.

The communications between the base device and the system 10 are preferably carried out over a secure connection utilizing for example, 128-bit encryption. Additionally, a private (non-public) communication may be provided by the system as a communication means between the system 10 and the base device as is known in the art. --